FUTURE VOTES

A SUMMARY OF FINDINGS FROM A WORKSHOP ON CYBERSECURITY, DISINFORMATION, AND ELECTION INTEGRITY

UNIVERSITY OF TORONTO

SCHWARTZ REISMAN INSTITUTE FOR TECHNOLOGY AND SOCIETY

the dais

Toronto Metropolitan University

ROGERS cybersecure catalyst

ABOUT US

SCHWARTZ-REISMAN INSTITUTE FOR TECHNOLOGY AND SOCIETY (SRI)

Founded in 2019, the Schwartz Reisman Institute for Technology and Society convenes a strong, multidisciplinary, and resourceful network of researchers focused on making significant strides in understanding—and influencing—the impact of powerful new technologies like AI on today's world.

THE DAIS AT TORONTO METROPOLITAN UNIVERSITY

The Dais is Canada's platform for bold policies and better leaders. The Dais is a public policy and leadership think tank at Toronto Metropolitan University, working at the intersection of technology, education, and democracy to build shared prosperity and citizenship for Canada.

ROGERS CYBERSECURE CATALYST

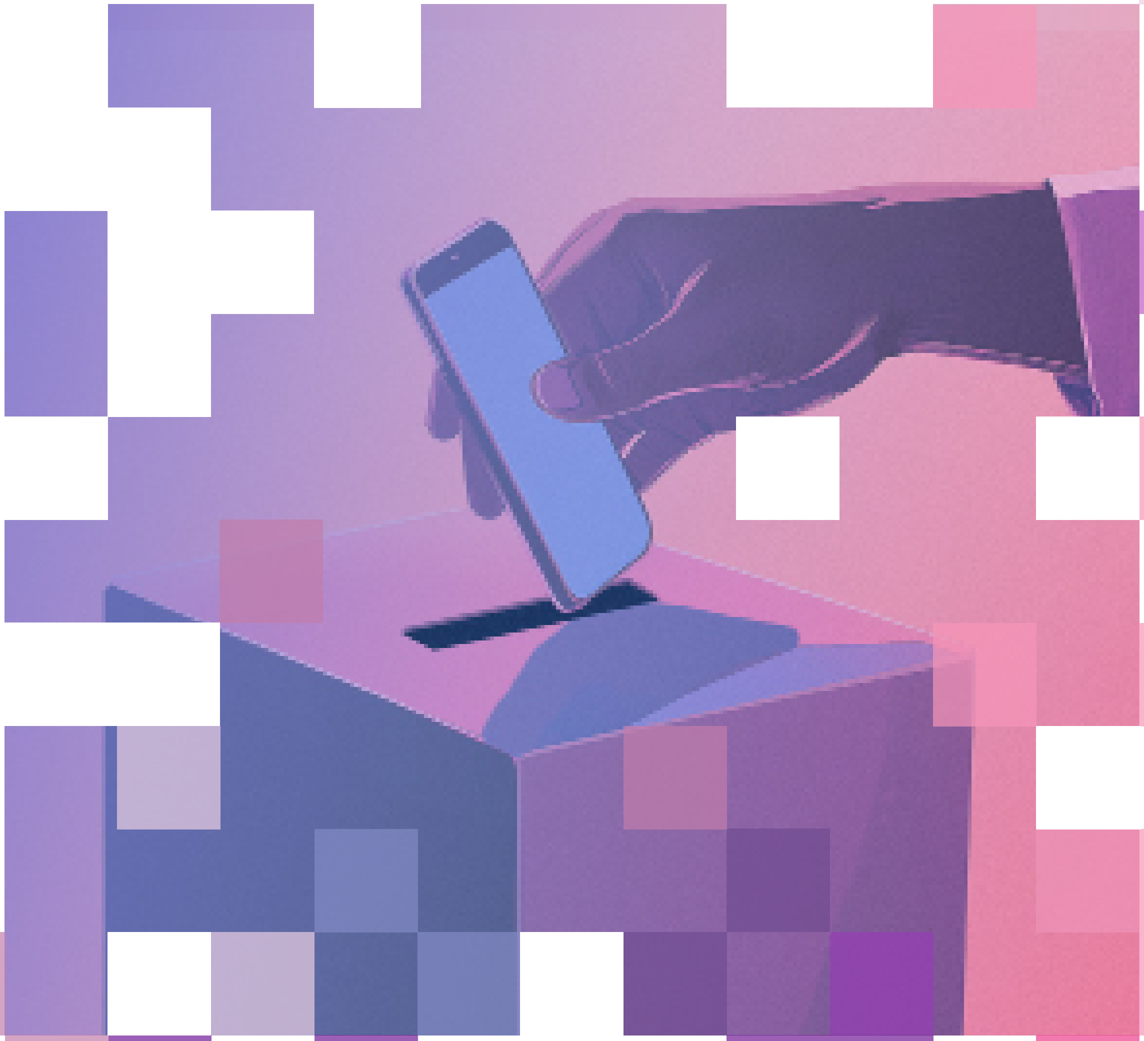
Rogers Cybersecure Catalyst holds an international reputation as a major global hub for cybersecurity training, entrepreneurship, research, policy development, and public education. The Catalyst offers a wide array of programs for individuals, entrepreneurs, and organizations of all sizes. Based at Toronto Metropolitan University, with our headquarters in Brampton, Ontario, Canada, the Catalyst delivers programs and services throughout Canada and around the world.

CONTENTS

ABOUT THIS PROJECT

FUTURE VOTES: A SUMMARY OF FINDINGS FROM A WORKSHOP ON CYBERSECURITY, DISINFORMATION, AND ELECTION INTEGRITY

This report is a reflection of findings from an event held in October 2024 in Toronto, Ontario by the Schwartz Reisman Institute for Technology and Society, the Dais, and Rogers Cybersecure Catalyst. The closed discussion was designed to bring together key cybersecurity and disinformation experts to explore how well-positioned governments are to respond to ongoing and future election-related security concerns. It included two sessions, beginning with a conversation focused on cyber threats to election infrastructure, followed by a discussion on the information ecosystem around elections. This report is a reflection of key insights shared during the event from experts in attendance across government, academia, industry, and the nonprofit sector.



INTRODUCTION

2024 was a landmark election year. Nearly two billion people voted across 70+ national elections, amounting to nearly half of the world's population.[1,2] Now, in 2025, with federal and provincial elections on the horizon, Canadians will face critical electoral decisions about the country's leadership and policy direction during a time of uncertainty and rapid change. Free and fair elections are a cornerstone of democracy. Elections have evolved alongside broader digitization, integrating technology into their administration. While this shift offers opportunities for greater accuracy and efficiency, it also transforms core roles. Election officials, for instance, have evolved from managing manual processes to navigating the modern complexities of digital systems. This growing reliance on technology coincides with an increasing prevalence of digital threats.

Elections have always faced challenges, but the digital era has introduced new obstacles, such as cyber threats, while significantly amplifying the scale and impact of others, like the spread of disinformation in online environments. Not only do these threats undermine the right of voters to engage in an electoral system free from coercion, but they erode public confidence and trust in democracy. Modern threats and disruptions present unprecedented challenges given the rise of artificial intelligence (AI). Elections are deeply social and collective mechanisms in democracies, which require a pragmatic and proactive response to ensure the protection of the values and institutions that matter most to society. In today's evolving threat landscape, are democratic governments prepared to defend against cyber threats that target election infrastructure and how will they counter disinformation campaigns?

This is a question we sought to address in October 2024 through the Future Votes workshop, co-hosted in Toronto, Ontario by the Schwartz Reisman Institute for Technology and Society, the Dais, and Rogers Cybersecure Catalyst. The closed discussion was designed to bring together 50+ cybersecurity and disinformation experts to explore how well positioned governments are to respond to election-related security concerns. It included two sessions, beginning with a conversation focused on the impact of cyber threats on election infrastructure, followed by a discussion about mis- and disinformation around elections. This report is a reflection of key insights shared during the event from experts in attendance across government, academia, industry, and the nonprofit sector.

ELECTION INFRASTRUCTURE AND CYBERSECURITY

Election infrastructure is made up of integrated systems, which are designated as critical infrastructure. According to the Cybersecurity & Infrastructure Security Agency (CISA), "this designation recognizes that... election infrastructure is of such vital importance to the way of life that its incapacitation or destruction would have devastating effects on the country." [3]

This election infrastructure includes but is not limited to:

- Voter registration databases
- IT systems including: counting, auditing, displaying election results, and post-election reporting to certify and validate results
- Voting systems and related infrastructure

Despite its critical importance, election infrastructure remains vulnerable to infiltration by multiple different threat actors. This makes it essential to isolate unique tactics and motivations to effectively address potential risks. State-sponsored cyber threat actors operate on behalf of nation-states, using sophisticated cyber activities to advance geopolitical objectives and in some cases, pursue financial gains. They do so through espionage which targets governments, organizations, and individuals. Cybercriminals are driven primarily by financial motives. They operate with varying levels of sophistication, increasingly leveraging accessible online markets to execute more complex campaigns.

Hacktivists, on the other hand, tend to be driven by ideological motivations. They typically operate with less sophistication than state-sponsored actors but can significantly impact an individual or organization's reputation through their activities. Insider threats originate from individuals within organizations who have access to internal networks and systems, often acting independently or in collaboration with other types of threat actors.

Cybersecurity is a significant global challenge affecting all sectors; in Canada, a number of recent, high profile attacks[4] point to crisis levels. In the context of elections, investing in comprehensive cybersecurity protections is especially critical. Elections rely on secure infrastructure to ensure voter data is safeguarded, ballots are accurately cast and counted, and election outcomes reflect the will of the people. Effective cybersecurity measures act as a critical defense against potential threats, not only to prevent breaches but also to ensure the electoral process remains resilient and reliable for future generations. The sophistication of today's cyber threat landscape means that attacks on people and institutions are no longer a matter of possibility—they are an inevitability. This shift emphasizes the critical need for robust defenses to reduce vulnerabilities and mitigate risks.

Beyond direct threats, cybersecurity also helps to foster public trust and confidence in the long-term integrity of the electoral process. Cybersecurity is not just a defensive measure or technical safeguard—it is a proactive investment in the future of democracy. In an era where cyber threats are a persistent reality, prioritizing election cybersecurity is both a necessary and prudent step to preserve the democratic process.

Traditionally, election infrastructure relied on human processes, physical ballots, and manual counting. Today, we are in the midst of transformation,[5] with varying levels of progress across regions ;resource-rich provinces continue to advance, while smaller municipalities and less-resourced provinces face challenges in modernizing at the same pace. Recognizing these variations is essential to understanding the full landscape, as election infrastructure is not fully digital across the country. With increased reliance on technology at each layer of the election infrastructure comes heightened cyber vulnerability. Collectively ensuring the security of this evolving infrastructure is central to safeguarding our democratic processes.

PRIORITIZING CYBERSECURITY FOR ELECTIONS

Safeguarding elections requires deliberate prioritization of infrastructure cybersecurity by government bodies. British Columbia provides a practical roadmap for other provinces and nations with respect to election security. In its recent provincial election, BC implemented a comprehensive technical strategy, assembling a dedicated security team to enhance resilience and protect electoral processes. Starting at the individual level, BC implemented protections to the administrative environment by restricting employee access to essential information and applying strict identity management protocols to monitor and control access to systems and servers. This security model was applied consistently across the province, including all 93 electoral offices, supported by advanced threat protection tools and secure VPN environments. BC also prioritized a key focus on partnership activities. They built new partnerships with federal and provincial bodies who monitored threats to election infrastructure and provided cyber hygiene guidance. Additionally, they established collaboration with private sector partners, such as big tech firms, who provided access to expert resources and continuous communication with cybersecurity advisors to prepare for potential breaches or attacks. These partnerships enabled proactive system testing, the development of checklists and protocols, and ensured that expert support was readily available in the event of a compromise.

British Columbia's electoral system highlights the pressing need to address the intersection of interests and capabilities shared between the public, private, and academic sector. Efforts to effectively safeguard cybersecurity and election infrastructure do not happen in isolation; other players, like technology companies, can play a transformational role in supporting election bodies to cultivate knowledge about digital security and identify cyber threats. In one case, big tech firms collaborate with election officials to build secure and resilient election infrastructure, offering tools and services designed to address key challenges in the election ecosystem. Such resources included, affordable cybersecurity solutions for campaigns, training for election officials on threat detection and resilience, content integrity tools to authenticate media, and intelligence support through expert analysis of threats. Additionally, they provide operational support during elections, such as situation rooms for threat response, and public awareness initiatives to promote informed voting.

SAFEGUARDING ELECTION CYBERSECURITY: PRACTICAL STEPS FOR POLICYMAKERS

In order to safeguard the cybersecurity of election infrastructure, policymakers can take various steps:

1. LEVERAGE THE BENEFITS OF COLLABORATION

A secure election system requires collaboration among diverse stakeholders, including private companies, election bodies, political parties, and representatives from infrastructure and software sectors, to facilitate information and resource sharing. Federal and provincial election authorities should be in conversation with national bodies like the Canadian Centre for Cybersecurity, the Canadian Security Intelligence Service (CSIS), and the Royal Canadian Mounted Police (RCMP), as well as garnering expertise from private sector partners and other cybersecurity advisors.These groups bring critical tools, training opportunities, and perspectives that can collectively enhance election security. Collaborative efforts should focus on:

- **Cybersecurity Best Practices**: Develop and share guidelines for responding to threats and safeguarding critical infrastructure, building off of globally-recognized standards from bodies like ISO and NIST.
- **Threat Monitoring and Tracking**: Form teams and strengthen relationships between public and private actors to identify, mitigate, and address emerging risks. Threat monitoring should be a practice that occurs regularly and takes place before, during, and after election periods.
- **Election Financing Transparency**: Establish clear guidelines for how private industry can work with election bodies and campaigns to ensure both flexibility and transparency around election financing.

The creation of multi-stakeholder forums to facilitate ongoing dialogue, knowledge sharing, and coordinated action could be a first step towards leveraging the benefits of collaboration.

2. PRIORITIZE PREPAREDNESS IN CAMPAIGN PLANNING

Election security should not be an afterthought. Mandating cyber action plans as part of campaign preparation can ensure political parties integrate security measures from the outset. A culture of cybersecurity must become second nature, with all actors equipped to manage risks. As one expert put it: “you don’t want to trade business cards in a hurricane.”

A practical first step is the creation of frameworks that require campaigns to include cybersecurity in their operational planning, with incentives for compliance.

3. UTILIZE REGULATION AS A STRATEGIC TOOL

Effective legislation can empower federal agencies to act decisively. Examples like Bill C-70—which eased restrictions on information sharing between CSIS and election authorities—and updates to the Security of Information Act, illustrate how regulatory adjustments can close gaps in the system.

This signals the importance of regularly reviewing and updating laws to reflect evolving cyber threats and empower agencies to protect electoral processes effectively.

4. ENHANCE PUBLIC AWARENESS THROUGH EDUCATION

Even with the most comprehensive protocols and practices in place, elections are ultimately a human endeavor, meaning humans remain the biggest vulnerability. Public understanding of election security is crucial to fostering trust. Through increasing knowledge and awareness, the government can equip citizens to recognize and respond to potential threats. This gives individuals agency in safeguarding democracy.

The launch of public education campaigns could be used to highlight the importance of election security, provide resources to identify threats, and promote digital literacy.

By implementing these strategies, the government can strengthen election cybersecurity, enhance protection of democratic processes, and build trust in the integrity of the electoral system.

THE INFORMATION ECOSYSTEM AROUND ELECTIONS

The Canadian Digital Media Research Network (CDMRN) defines the information ecosystem as "The sum of complex but analyzable set of relationships found in and across digital media . . . composed of interconnected but distinct communities across social and traditional media."[6] More simply, our information ecosystems encapsulate both the content and the infrastructure that enables information sharing in our daily lives, through journalism, news, and social media, and how it flows through users and their networks.

The ecosystem is dynamic, shaped by the cultural context of the platform and users' engagement, while in turn shaping discourse in reaction to events or issues. We have never been more connected due to digital technologies, meanwhile levels of polarization and information silos are increasingly apparent both online and offline.[7]

Users' interactions with the information ecosystem are informed by their levels of media literacy.[8] Since everyone has the ability to contribute to the information ecosystem, there are limited systems in place to vet the accuracy or validity of the type of content shared. It's no surprise then that malicious actors take advantage of this and manipulate both the content and infrastructure that supports our information sharing capacities, in order to incite mistrust and spread disinformation. Election periods are not the only critical moment where nefarious actors want to have influence; authoritarian governments especially exploit non-election periods to create and disseminate false narratives over time to challenge the integrity of the information ecosystem in democracies.

BEHIND A POLLUTED INFORMATION ENVIRONMENT

With the rise of synthetic [artificially generated] images and text, deepening political polarization, and the growing threat of mis- and disinformation,[9] people have become wary of the information they encounter. In the face of an overwhelming volume of information within a rapidly shifting environment and the absence of reliable fact-checking mechanisms, the public can grow weary of discerning credible sources from falsehoods. For certain communities, especially those living in the diaspora, obstacles such as language barriers make accessing reliable information and distinguishing credible sources from misinformation particularly challenging, which leaves them more vulnerable to disinformation campaigns. This has tremendous consequences for our national security, the integrity of our democratic processes and institutions, and the foundations of public trust.

There are a range of malicious actors in the information ecosystem, aiming to incite rage, foster mistrust, and weaken democracies. Domestic extremists may be motivated to bring about political change in favour of their political candidates. Authoritarian states may exploit their actions disrupting political processes abroad to reinforce narratives domestically, using foreign instability as a comparison to suppress dissent and discourage criticism of their own governance. Social media platforms, from private messaging apps like WhatsApp and Signal, to social media outlets like X (formerly Twitter) and Facebook can be ideal vehicles to disrupt the information ecosystem. In particular, private messaging apps play a key role in facilitating cross-border political interactions. As such, platforms play a critical role in moderating content, ensuring malicious actors are not creating fake profiles or proliferating bots to fulfill their objectives, and that the public has adequate mechanisms to flag or report content. While mis- and disinformation are not new phenomena, social media platforms have supercharged the speed and distance with which information—both accurate and false—can travel.

The means for individuals to spread disinformation are currently simple and cheap to enact. Whether a user wishes to share false information via their own social media platforms, or purchase disinformation-for-hire, the impact of disinformation on credibility and reputation are lasting and often irreversible. While there are various platform, regulatory, and user responses that can be taken, building user resilience against disinformation must first be done through building public trust.

SAFEGUARDING THE ELECTION INFORMATION ECOSYSTEM: PRACTICAL STEPS FOR POLICY-MAKERS

In order to safeguard the information ecosystem surrounding elections, policymakers can take various steps:

1. **LEVERAGE REGULATION THOUGHTFULLY**

Regulation can be a powerful tool, but its design must account for the complexity of safeguarding election security. Blunt, one-size-fits-all approaches risk unintended consequences, such as missed nuances in application and disproportionate impacts for underrepresented groups. Recent examples, such as British Columbia's provisions on deception and comparable measures in U.S. states, demonstrate how tailored policies can address specific challenges. These laws emphasize the need for nuanced solutions that balance the right to reliable information with protections against misuse.

This can be accomplished by:

- Conducting supporting research to explore legal frameworks for guaranteeing access to reliable information without infringing on rights.
- Developing legislation that narrowly targets deceptive practices while ensuring flexibility to adapt to emerging threats.
- Exploring the feasibility of "safe harbour" provisions to protect platforms, researchers, or organizations that act in good faith to combat disinformation.

2. **INVEST IN EVIDENCE-BASED RESEARCH AND MOBILIZE FINDINGS**

Critical, community-engaged research can provide valuable insights into effective interventions, particularly in vulnerable communities. This work should be supported by efforts to mobilize academic findings into actionable outputs that reach diverse audiences. Steps to accomplish this could look like the following:

- Increasing funding for applied research focused on community engagement to identify when and how to intervene against disinformation.
- Supporting the translation of findings into accessible formats (e.g., videos, infographics, or guides) tailored to specific audiences, including policymakers, community leaders, and the general public, as well as providing these materials in a wider variety of translated texts to ensure inclusivity and broader reach.

3. **STRENGTHEN INFORMATION-SHARING MECHANISMS**

Effective cross-sectoral information sharing is essential to ensure a proactive response. Coordination among entities such as the RCMP, CSIS, and the Centre for Cybersecurity can ensure that risks are identified and mitigated swiftly. Beyond these entities, it is also paramount to establish regular briefing sessions with political parties regarding risk identification and issue response. This would involve:

- Developing robust frameworks for inter-agency collaboration, including secure channels for sharing sensitive information.
- Expanding programs like Elections BC's to a national scale, ensuring all political parties, campaigns, and candidates are informed about evolving threats.

4. PRIORITIZE PUBLIC EDUCATION FOR LONG-TERM RESILIENCE

Building public resilience requires a sustained focus on digital, media, and information literacy. However, this must align with Canada's unique systems and structures, creating a tailored approach that equips citizens to navigate the information ecosystem effectively. To do this, policymakers could:

- Develop a Canadian-specific strategy for public education on digital literacy, leveraging partnerships with educators, libraries, and media organizations.
- Create multi-pronged literacy campaigns that address disinformation, critical thinking, and online safety to empower citizens as active defenders of democracy.

By integrating thoughtful regulation, fostering evidence-based research, enhancing information-sharing, and investing in public education, the government can create a multi-layered approach to protect the information ecosystem for election security that safeguards democratic processes and bolsters public trust.

CONCLUSION

Elections are a cornerstone of democratic systems. Yet, the distinction between election and non-election cycles is increasingly blurred, a phenomenon known as the "permanent campaign." The integrity of our democracies are more vulnerable than ever, with the greatest concern being the erosion of trust in democratic processes and institutions. While technology has amplified threats to election integrity, it also offers powerful tools to defend democracy. Above all, protecting elections is a shared responsibility that requires collaboration among stakeholders to combat mis/disinformation, share expertise to mitigate cyber threats, and build on each other's efforts to safeguard democratic processes.

REFERENCES

[1] Koh Ewe and Chad De Guzman, “Midway through the Ultimate Election Year: How the World Has Voted so Far,” TIME, July 1, 2024, https://time.com/6991526/world-elections-results-2024/

[2] International IDEA, “The 2024 Global Elections Super-Cycle,” https://www.idea.int/initiatives/the-2024-global-elections-supercycle

[3] Cybersecurity & Infrastructure Security Agency, “Election Security,” 2024, https://www.cisa.gov/topics/election-security

[4] Canadian Centre for Cyber Security, “National Cyber Threat Assessment 2025-2026,” 2024, https://www.cyber.gc.ca/en/guidance/national-cyber-threat-assessment-2025-2026#wb-tphp

[5] Elections Canada, “Digital transformation and investment plan: CEO appearance on the Main Estimates 2023-2024 before the Standing Committee on Procedure and House Affairs,” October 31, 2023, https://www.elections.ca/content.aspx?section=abo&dir=comp/may1823&document=p7&lang=e

[6] The Canadian Digital Media Research Network, The Media Ecosystem Observatory, and the Project on Information Ecosystem Resilience, “Information Incident Response Protocol,” September, 2024, https://static1.squarespace.com/static/65427f5b140649321cd829e9/t/66f1c0b68793bb3f19773ab8/1727119542450/Incident+Response+Protocol+-+v2+Public.pdf

[7] Justin Ling, “Far and Widening: The Rise of Polarization in Canada,” Public Policy Forum, August 2023, https://ppforum.ca/wp-content/uploads/2023/08/TheRiseOfPolarizationInCanada-PPF-AUG2023-EN2.pdf

[8] Evan F. Kuehn, “The information ecosystem concept in information literacy: A theoretical approach and definition,” Journal of the Association for Information Science and Technology 74, No. 4 (December 23, 2022), https://asistdl.onlinelibrary.wiley.com/doi/10.1002/asi.24733

[9] Elections Ontario, “Maintaining a Level Playing Field: Addressing Misinformation and Disinformation Threats to Electoral Administration in Ontario,” October, 2024, https://www.elections.on.ca/content/dam/NGW/sitecontent/2024/reports/Maintaining%20a%20Level%20Playing%20Field%20-%20Addressing%20Misinformation%20and%20Disinformation%20Threats%20to%20Electoral%20Administration%20in%20Ontario.pdf